REMARKS

Claims 1-5, 7-9, 11-13, 15 and 16 are pending in this application, and, in the Final Office Action, the Examiner finally rejected all of these claims under 35 U.S.C. 102(e) as being fully anticipated by U.S. Patent 6,237,095 to Curry, et al. (Curry).

The rejection of the claims under 35 U.S.C. 102(e) in view of Curry is respectfully traversed for the reasons explained below. The Examiner is thus asked to reconsider and to withdraw the final rejections of claims 1-5, 7-9, 11-13, 15 and 16, in view of Curry under 35 U.S.C. 102(e), and to allow these claims.

As explained in detail in the present application, the instant invention provides a procedure to create and to use electronic cash. With a preferred embodiment of the invention, a customer sends to a bank a request for digital cash and a public key of an encryption scheme of the customer. The bank signs the cash using a secret key of the bank's own digital signature scheme, and encrypts the signature by using the public key provided by the customer. The bank also encrypts, using the public key given to the bank by the customer, an unsigned copy of the cash. A copy of the encrypted signed cash and a copy of the encrypted unsigned cash are both sent to the customer by the bank.

The customer then decrypts both of these copies – that is, both the signed and unsigned copies of the cash - by using the private key of the customer's encryption scheme. The customer then uses this decrypted, signed and unsigned pair of copies for payment to a third party. The third party, using these decrypted signed and unsigned copies of the cash, can then ask the bank to confirm the validity of the digital cash. If that validity is confirmed, this third party is able to redeem the digital cash for payment.

An important feature of the present invention is that the bank encrypts both the signed and unsigned copies of the digital cash using the public key of the customer's encryption scheme – that is, the customer has the private key of that encryption scheme. Then, both encrypted copies – that is, the encrypted copy of the signed coin and the encrypted copy of the unsigned coin - are sent back to the customer. Because of this feature, the customer, and only the customer, is able to decrypt both the signed and unsigned copies of the digital cash by using the private key of the customer's encryption scheme. In this way, only the customer is able to control the use of these copies.

Neither Curry nor the other prior art of record disclose or suggest this feature of the present invention.

In particular, Curry describes an electronic module used for secure payment, and is particularly directed to communicating encrypted information between the module (preferably portable), and a service provider's equipment. The module has a unique identification capable of creating a random number, e.g., a SALT, and passing the random number along with a request to exchange money to a service provider's equipment. The service provider's equipment encrypts the random number with a public of private key , and along with other information passes the encrypted information to the module as a signed certificate. The module decrypts the certificate and compares the encrypted number with the original random number, where if the same, the procedure is deemed secure. The module may time stamp and store information in memory relating to the transaction.

While the Examiner states in the Office Action that the cited text at col. 8, lines 8-43 discloses, among other matters, sending back to the payee or user both the encrypted copy of the signed coin ("certificate") and the encrypted copy of the unsigned coin ("certificate"). But our

careful review finds that Curry's cited text does not disclose sending these two encrypted coins/certificates back to the payee/user. In particular, this section of Curry shows that only a money amount and SALT are encrypted and sent as a signed certificate/coin to the payee/user. There is no teaching, though, of sending encrypted copies of two coins/certificates, - one signed by the bank and one unsigned by the bank – to the user.

In particular, the problem addressed by Curry at lines 8-43 of col. 8 concerns "replay" or "duplication" of digital certificates representing cash. Curry states that a receiver of a payment must take special steps to insure that the digital certificate he receives is not a replay of a previously issued certificate. The col. 8 text states that the Curry method is a SALT method, whereby a random number is sent and used in a challenge/response mode. That is, the other party is challenged to return the random number sent as part of that party's response. The payer or bank constructs a signed certificate, which includes both the money amount and the payee's SALT. The payee or user decrypts the signed certificate upon receipt, and confirms that the SALT is the same as was provided. Only the signed certificate is encrypted and returned to the user/payee by the bank/payer. Nowhere does the cited Curry text teach or suggest that the payer/bank sends both an encrypted signed certificate and an encrypted unsigned certificate, as do each of applicants' independent claims 1, 3, 7 and 11, and the claims which depend therefrom.

Independent Claims 1, 3, 7 and 11 clearly describe important features of this invention that are not shown in or suggested by Curry. In particular, Claims 1 and 7 describe the features that encrypted copies of the signed and unsigned coins are encrypted using the public key of an encryption scheme, that both of these copies are sent back to the user or customer, and that the user or the customer uses the private key of this encryption scheme to decrypt both the signed

and unsigned copies of the coin. Claims 1 and 7 also describe the feature that the user or customer uses that pair of coins - that is, the signed and unsigned copies of the coin - as digital cash. Claim 7 add the further limitation that this pair of coins is used as a payment to a recipient.

Claims 3 and 11, as presented herein, describe the features that the secure cryptography generator encrypts both the signed unit and the unsigned unit using the public key of the given encryption scheme communicated to the cryptography generator from the customer. As further described in these claims, this pair of encrypted coins are transmitted back to the customer, decrypted by the customer, and used as a unit as payment to a recipient, and this recipient then presents this pair of coins to the bank for credit.

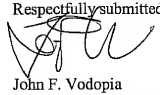
The other references of record have been reviewed, and these other references, whether considered individually or in combination, also do not disclose or suggest encrypting the pair of coins, or this use of the pair of subsequently decrypted signed and unsigned coins, as described in claims 1, 3, 7 and 11.

In light of the differences between claims 1, 3, 7 and 11 and the prior art, and because of the advantages associated with those differences, these claims patentably distinguish over Curry and the other prior art and are allowable. Claim 2 is dependent from claim 1 and is allowable therewith; and claims 4, 5, 15 and 16 are dependent from claim 3 and are allowable therewith. Also, Claims 8 and 9 are dependent from claim 7 and are allowable therewith; and claims 12 and 13 are dependent from, and are allowable with, claim 11.

For the reasons discussed above, the Examiner is asked to reconsider and to withdraw the final rejections of claims 1-5, 7-9, 11-13, 15 and 16 under 35 U.S.C. 102(e) in view of Curry, and to allow these claims. If the Examiner believes that a telephone conference with Applicants'

Attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,



John F. Vodopia
Registration No. 36,299
Attorney for Applicants

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza - Suite 300
Garden City, New York 11530
(516) 742-4343

JFV:gc